JAMES RENKEN

UNIVERSAL ATTACK SURFACES

This talk assumes basic knowledge of DNS, SSL/TLS, and networks. I won't go deeply into algorithms, code, or demos.

Be excellent to each other.

James P. Renken, PLLC

I’m just an experienced generalist. I’ve also been professionally trained to sound authoritative. Trust no one.

This is not legal advice!

- Third-party Web sites
- Government (executive & judicial)
- Telephone companies
- Postal service
- Financial institutions
- Domain registrars
- E-mail correspondents
- DNS relying parties
- SSL/TLS relying parties
- The actual Internet

If you're not using

Have I been pwned?

You're doing it wrong.

- Content Security Policy (CSP)
- Sub-Resource Integrity (SRI)

Corporate identity theft: it's a thing. (c. 2006)

- Most information is public—sometimes even signatures
- Difficult to prosecute

- Keep your filings up to date
- Monitor your entity's status, business credit & court records
- Watch for entities with similar names

Resource: BusinessIDTheft.org

WANTED

By U.S. MARSHALS

Name: CEGLIA, Paul

Alias: SEGLIA, Dean

DATE OF PHOTO: 10/26/2012

Sex..... MALE

Race..... WHITE

Height..... 5'10"

Weight..... 195 pounds

Eyes..... BROWN

Hair..... BLACK

Marks/Scars/Tattoos..... NONE

Wanted For..... WIRE FRAUD

Warrant Issued By..... W/New York

Date of Warrant..... March 8, 2015


I have an annuity but I need cash now.

Lawyer accused of forging signatures of seven Broward judges

By **Rafael Olmeda · Contact Reporter**
Sun Sentinel

FEBRUARY 22, 2016, 6:40 PM

A Miami lawyer is facing multiple forgery charges after investigators found he forged the signatures of seven different Broward County and Circuit judges on documents related to civil cases involving structured settlements, according to court records.

Jose Manuel Camacho was arrested in October after Broward County Judges Marina Garcia-Wood and Carlos Rodriguez found their forged signatures on legal documents filed with the clerk of courts.

After the judges complained, Broward Sheriff's Detective John Calabro interviewed them and five other judges. In all, Camacho, 46, was accused of forging 114 signatures. The other judges were Eileen

- Social engineering vs. telco
- Social engineering vs. subscriber
- VoIP vulnerabilities
- Local Number Portability (LNP)
- Wiretaps
- SS7 attacks

- Talk to your telco: activate extra security
- Secret numbers for sensitive uses

deray mckesson @deray · 7h

I was hacked today: my Twitter account, two email addresses, & my phone. It was not due to passwords, they hacked my phone account itself.

946 707

deray mckesson

@deray

Following

At 10:31 am, someone called @verizon impersonating me and successfully changed my SIM & unsuccessfully attempted to change my phone number.

RETWEETS	LIKES
619	329

2:46 PM - 10 Jun 2016

619 329

deray mckesson
@deray

Following

They simply needed to last four digits of my social security number to gain full access to my @verizon account.

> **Kona** @Kona99
>
> @deray What information did that hackers provide to Verizon in order to gain access to your accounts?

RETWEETS 115 LIKES 86

2:56 PM - 10 Jun 2016

115 86

- Forwarding fraud
- Outside theft
- Inside theft

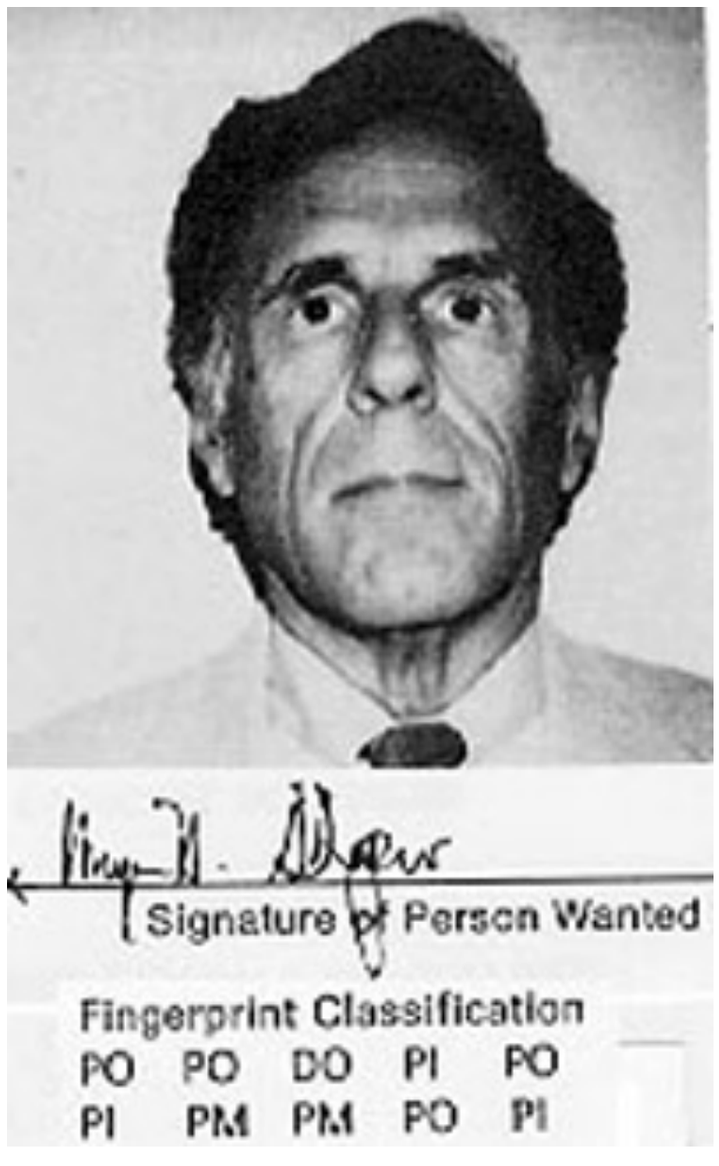
- USPS Caller Service (~ $75-120/month)
- Secret addresses for sensitive uses

Resource: USPS “Best Practices for Mail Center Security”

WANTED

U.S. POSTAL INSPECTION SERVICE

Myron Herbert Shapiro



Violations: Mailing of Obscene Material 18 USC 1461, Wanted on Federal Arrest Warrant for unlawful flight to avoid prosecution, 18 USC 1073.

Case No.: 666-0289012-PMO(2)

NCIC No.: W629611258

FBI No.: 451456NA4

Warrant No.: 9167-0409-0042-B, March 20, 1991, Middle District of PA

Aliases: none

DOB: 05/08/26, New York

Description: Caucasian Male, 5’11”, 168 lbs., brown hair, brown eyes

Misc. Info.: Passport No. 042158770. Self-Employed Businessman. Flight Risk, known to travel to Europe, Israel and Caribbean Islands. Subject may have fled to another country. Please refer to INTERPOL.

- Document forgery / social engineering
- Check fraud
- Automated Clearing House (ACH) fraud

- Positive Pay
- Sweep accounts
- Monitor your business credit

- Document forgery / social engineering
- Uniform Domain-Name Dispute-Resolution Policy (UDRP)
- Court orders

- Keep WHOIS data up to date & monitor contact addresses
- Monitor your domains' status
- Use a good registrar
- Use two-factor authentication
- Talk to your registrar: activate extra security

Resource: ICANN SSAC Report

"By simply Base64 encoding an .as domain name and appending it to an URL on the nic.as website, it was possible to view the entire domain record for the domain (including unencrypted passwords for domain owners, technical contacts, and billing contacts)."

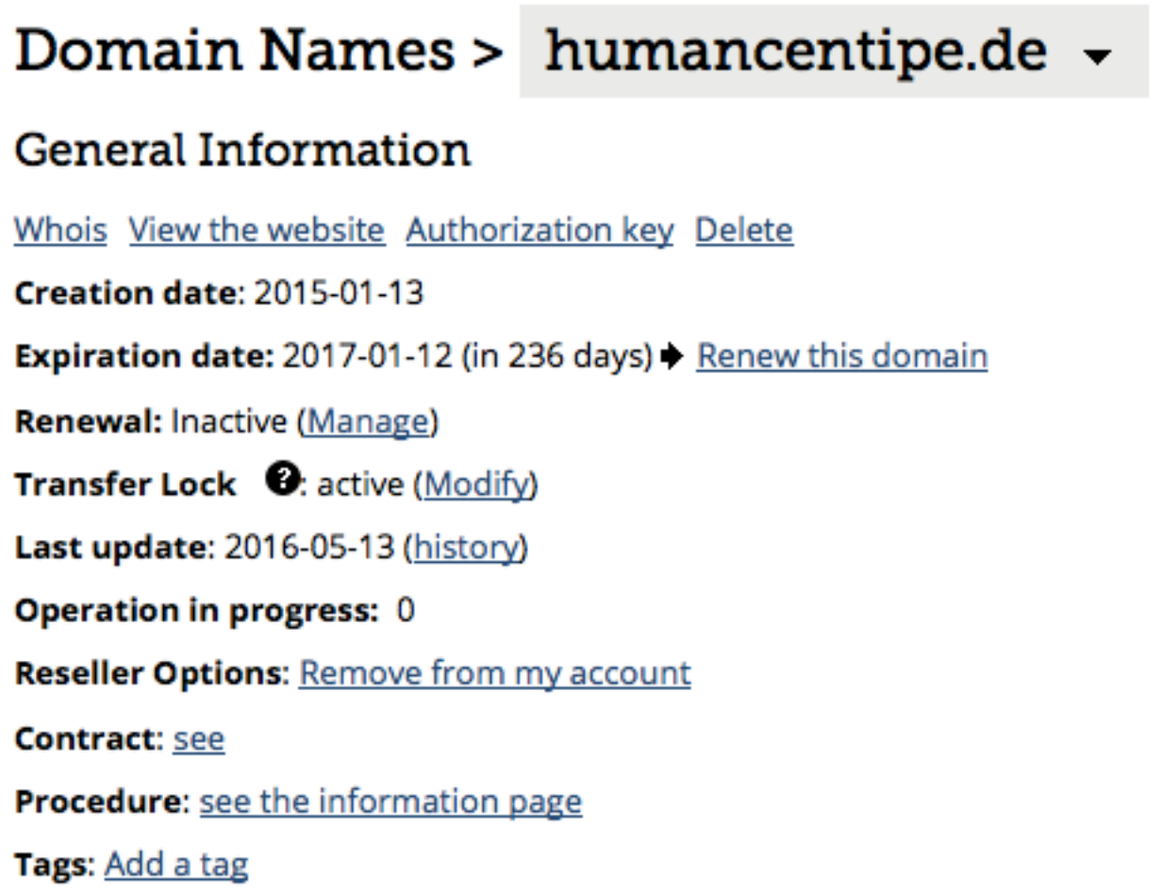
- InfoSec Guy

- 21st January 2016 09:13 – Responsible disclosure to AS Registry
- 23rd January 2016 07:03 – AS Registry "noted" concern, but dismissed severity
- 24th February 2016 19:31 – AS Registry report flaw has been resolved & customers in the process of being notified

- Simple forgery
- Typosquatting
- Small hosts with naive e-mail routing

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain Message Authentication Reporting & Conformance (DMARC)
- Talk to your correspondents

- Typosquatting
- Bitsquatting
- DNS request hijacking



- Monitor domain registrations
- Protective domain registrations
- Domain Name System Security Extensions (DNSSEC)

Resources: TypoFinder; DNSSEC.NET; DNSSEC Analyzer; DNSViz

- SSL/TLS stripping
- Trick a certificate authority
- Hack a certificate authority
- Be a certificate authority

- HTTP Strict Transport Security (HSTS)
- DNS-based Authentication of Named Entities (DANE)
- Monitor Certificate Transparency (CT) logs

Resources: HSTS Preload Submission; report-uri.io; Censys

- HTTP Public Key Pinning (HPKP) - careful now


©ARCHIE McPHEE

- Privileged network positions
- Border Gateway Protocol (BGP) hijacking

- Use mandatory end-to-end encryption
- Monitor your routes
- Monitor & participate in the network operations community
- Resource Public Key Infrastructure (RPKI)

Resources: BGPmon; NANOG Mailing List; puck.nether.net

james@sandwich.net
@jrenken